

By Debra Littlejohn Shinder, MCSE, MVP

We all do dumb things now and then, and computer users are no exception. Inadvertently pressing the wrong key combination or innocently clicking OK in the wrong dialog box can change important settings that alter a computer's behavior or even crash the system.

Nervous newbies are often fearful that one wrong move might break the computer forever. Luckily, short of taking a sledge hammer to the box, the consequences aren't usually quite that dire. Even so, users often do create problems for their computers and for your network. Here's a description of common missteps you can share with your users to help them steer clear of preventable problems.

## 1 Plug into the wall without surge protection

Here's one that actually *can* physically destroy your computer equipment, as well as the data it holds. You may think your systems are in danger only during an electrical storm, but anything that interrupts the electrical circuit and then starts the current back again can fry your components. Something as simple as someone turning on an appliance that's plugged into the same circuit (especially a high voltage one such as a hair dryer, electric heater, or air conditioner) can cause a surge, or a surge may be caused by a tree limb touching a power line. If you have a power outage, you may experience a surge when the electricity comes back on.

You can protect your systems against damage from power surges by always using a surge protector, but it's important to be aware that most cheap surge protectors will survive only a single surge and need to be replaced afterward. An Uninterruptible Power Supply (UPS) is better than a surge protector; it has a battery that keeps power flowing smoothly even when there's an outage, to give you time to gracefully shut down.

## 2 Surf the Internet without a firewall

Many home users plug their computers right into their spiffy new cable or DSL modems and hop onto the Internet without realizing that they're putting themselves at risk from viruses and attackers. Every Internet-connected computer should be protected by a firewall; this can be a firewall built into the broadband modem or router, a separate firewall appliance that sits between the modem/router and the computer, a server at the network's edge running firewall software, or personal firewall software installed on the computer (such as ICF/Windows Firewall built into Windows XP or a third-party firewall program like Kerio or ZoneAlarm).

One advantage of personal firewalls on laptop computers is that they're still with you when you take the computer on the road and plug into a hotel's DSL or cable port or connect to a wireless hotspot. Just having a firewall isn't enough, though. You must also be sure it's turned on and configured properly to protect you.

## 3 Neglect to run or update antivirus and anti-spyware programs

Let's face it: Antivirus programs can be a royal pain. They're always blocking some application you want to use, you often have to disable them to install new software, and they have to be updated on a regular basis to do any good. Seems like the subscription is always expiring and prompting you to renew it--for a fee, in many cases. But in today's environment, you can't afford to go without virus protection. The malicious programs that AV software detects--viruses, Trojans, worms, etc.--can not only wreak havoc on your system but can spread via your computer to the rest of the network. In extreme cases, they can bring down the whole network.

Spyware is another growing threat; these are programs that install themselves on your computer (usually without your knowledge) and collect information from your system that is then sent back to the spyware program's author or vendor. Antivirus programs often don't address spyware so it's important to run a dedicated spyware detection and removal program.

## 4 Install and uninstall lots of programs, especially betas

You like to be on the cutting edge, so you often install and try out new software. Beta programs are usually free and give you a chance to sample neat new features before most people. There are also many freeware and shareware programs made available as Internet downloads by their authors. We know you'd never do it, but some users even install pirated software or "warez."

The more programs you install, the more likely you are to run across ones that either include malicious code or that are poorly written and cause your system to behave improperly or crash. The risk is greater with pirated programs.

Even if you install only licensed, final-release commercial software, too many installations and uninstallations can gunk up the registry. Not all uninstall routines completely remove program remnants and at the least, this practice can cause your system to slow down over time.

You should install only the programs that you really need, stick with legitimate software, and try to minimize the number you install and uninstall.

## 5 Keep disks full and fragmented

One of the results of installing and uninstalling lots of programs (or adding and deleting data of any kind) is that it fragments your disk. Disk fragmentation occurs because of the way information is stored on the disk: On a new, clean disk, when you save a file it's stored in contiguous sections called clusters. If you delete a file that takes up, for example, five clusters, and then save a new file that takes eight clusters, the first five clusters' worth of data will be saved in the empty space left by the deletion and the remaining three will be saved in the next empty spaces. That makes the file fragmented, or divided. To access that file, then, the disk's read heads won't find all the parts of the file together but must go to different locations on the disk to retrieve it all. That makes it slower to access. If the file is part of a program, the program will run more slowly. A badly fragmented disk will slow down to a crawl.

You can use the disk defragmenter built into Windows (Programs | Accessories | System Tools) or a third-party defrag program to rearrange these pieces of files so that they're placed contiguously on the disk.

Another common cause of performance problems and application misbehavior is a disk that's too full. Many programs create temporary files and need extra free space on the disk to operate. You can use Windows XP's Disk Cleanup Tool or a third-party program to find and delete rarely used files, or you can manually delete files to clear space on your disk.

## 6 Open all attachments

Some folks just can't help themselves: Getting an e-mail message with an attachment is like getting an unexpected gift. You just *have* to peek inside to see what it is. But just as that package left on your doorstep could contain a bomb, that file attached to your mail message could contain code that will delete your documents or system folder or send viruses to everyone in your address book.

The most blatantly dangerous attachments are executable files--those that run code--with extensions like .exe, .cmd, and many others (see <http://antivirus.about.com/od/securitytips/a/fileextview.htm> for a list of file extensions for different types of executables). Files that aren't themselves executables, such as Word .doc files and Excel .xls files, can contain embedded macros. Scripts (Visual Basic, JavaScript, Flash, etc.) aren't directly executed by the computer but are run by other programs.

It used to be that you could assume plain text (.txt) or graphics (.gif, .jpg, .bmp) files were safe, but not anymore. File extensions can be "spoofed"; attackers take advantage of the Windows default setting that doesn't display common file extensions to name executables something like greatfile.jpg.exe. With the real extension hidden, it shows up as greatfile.jpg. So the recipient thinks it's a graphic, but it's actually a malicious program.

You should open attachments only when they're from trusted sources and only when you're expecting them. Even if the mail with the attachment appears to come from someone you trust, it's possible that someone spoofed their address or that their computer is infected with a virus that sent the attachment to you without their knowledge.

## 7 Click on everything

Opening attachments isn't the only type of mouse click that can get you in trouble. Clicking on hyperlinks in e-mail messages or on Web pages can take you to Web sites that have embedded ActiveX controls or scripts that can perform all sorts of malicious activities, from wiping your hard disk to installing a backdoor program on your computer that a hacker can use to get in and take control of it.

Clicking the wrong link can also take you to inappropriate Web sites that feature pornography, pirated music or software, or other content that can get you in trouble if you're using a computer on the job or even get you in trouble with the law.

Don't give in to "click mania." Think before you click a link. Links can also be disguised in "phishing" messages or on Web sites to appear to take you to a different site from the ones they really point to. For example, the link might say [www.safesite.com](http://www.safesite.com), but it actually takes you to [www.gotcha.com](http://www.gotcha.com). You can often find out the real URL by hovering over the link without clicking it.

## 8 Share and share alike

Your mother taught you that it's nice to share, but when you're on a network, sharing can expose you to dangers. If you have file and printer sharing enabled, others can remotely connect to your computer and access your data. Even if you haven't created any shared folders, by default Windows systems have hidden "administrative" shares for the root of each drive. A savvy hacker may be able to use these shares to get in. One way to prevent that is to turn off file and printer sharing--*if* you don't need to make any of the files on your computer accessible across the network. This is especially a good idea if you're connecting your laptop to a public wireless hotspot. You can find instructions on how to do so at <http://www.pcmag.com/article2/0,1895,1277222,00.asp>.

If you do need to make shared folders accessible, it's important that they be protected by both share-level permissions and file-level (NTFS) permissions. Also ensure that your account and the local administrative account have strong passwords.

## 9 Pick the wrong passwords

That brings us to another common mistake that can expose you to attacks: picking the wrong password. Even if you don't belong to a network where the administrator forces you to select strong passwords and change them regularly, you should do so. Don't pick passwords that are easy to guess, such as your birthdate, loved one's name, social security number, etc. Longer passwords are harder to crack, so make your password at least eight characters long; 14 is even better. Popular password-cracking methods use "dictionary" attacks, so don't use words that are in the dictionary. Passwords should contain a combination of alpha, numeric, and symbol characters for best security.

A long string of nonsense characters may create a password that's tough to crack, but if you can't remember it, you'll defeat the purpose by writing it down (where an intruder may be able to find it). Instead, create a phrase you can remember easily and use the first letters of each word, along with logical numbers and symbols. For example: "My cat ate a mouse on the 5<sup>th</sup> day of June" becomes "Mc8amot5doJ."

## 10 Ignore the need for a backup and recovery plan

Even if you follow all these suggestions, an attacker may crash your system or your data may be corrupted or get wiped out by a hardware problem. That's why it's essential that you always back up your important information and have a plan for recovering from a system failure.

Most computer users know they should back up, but many never get around to it. Or they make an initial backup but don't update it regularly. Use the built-in Windows backup program (Ntbackup.exe in Windows NT, 2000, and XP) or a third-party backup program and schedule backups to occur automatically. Store backed up data on a network server or removable drive in a location away from the computer itself, in case of a natural disaster like flood, fire, or tornado.


Remember that the data is the most important thing on your computer. The operating system can be reinstalled and so can applications, but it may be difficult or impossible to recreate your original data. (See ["10 ways to protect your data"](#) for additional suggestions.)

Nonetheless, you can save time and frustration by backing up your system information too. You can create mirror images of your disks using popular "ghost" or "clone" programs. This will allow you to restore the system quickly instead of going through the tedious installation process.



Debra Littlejohn Shinder is a technology consultant, trainer and writer who has authored a number of books on computer operating systems, networking, and security. These include *Scene of the Cybercrime: Computer Forensics Handbook*, published by Syngress, and *Computer Networking Essentials*, published by Cisco Press. She is co-author, with her husband, Dr. Thomas Shinder, of *Troubleshooting Windows 2000 TCP/IP*, the best-selling *Configuring ISA Server 2000*, and *ISA Server and Beyond*.

## Additional resources

- TechRepublic's [Downloads RSS Feed](#) 
- Sign up for TechRepublic's [Downloads Weekly Update](#) newsletter
- Sign up for our [Desktops NetNote](#)
- Check out all of TechRepublic's [free newsletters](#)
- ["10 ways to avoid being the victim of identity theft"](#) (TechRepublic download)
- ["10 ways to protect your data"](#) (TechRepublic download)
- ["10 common social engineering plays... and how to protect against them"](#) (TechRepublic download)

## Version history

**Version:** 1.0

**Published:** May 17, 2006

## Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team